MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 3, 2015/2016

TPB3141 – PASSWORD AUTHENTICATION AND BIOMETRICS

(All sections / Groups)

31 MAY 2016
2.30 p.m – 4.30 p.m
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This question paper consists of 8 pages, including the cover page, with 10 MCQs and 6 questions only.

2. Attempt **ALL** questions in **Section A.**

3. Attempt **FIVE out of SIX** questions in **Section B.** All questions carry equal marks and the distribution of the marks for each question is given.

4. Please print all your answers in the Answer Booklet provided.

SECTION A: Please attempt **ALL** multiple choice questions. [10 marks]

1. _____, also known as the CIA triad, is a model designed to guide policies for information security within an organization.
   a. Confidentiality, Identification and Authentication
   b. Confidentiality, Integrity and Availability
   c. Circumvention, Integrity and Assurance
   d. Circumvention, Identification and Assurance

2. Which of the followings is **NOT** related to Tokens?
   a. Very reliable identification.
   b. Medium typical deployment cost.
   c. Works with legacy systems.
   d. Sometimes requires client-side software.

3. Which of the followings is **NOT** belong to one of the types of Radio-Frequency Identification (RFID) transponders?
   a. Read Only (R/O)
   b. Read Write (R/W)
   c. Write Once Read Many times (WORM)
   d. Write Only (W/O)

4. _____ refers to an application of combining data from two or more biometric sensors, such as synchronized reflective-based and temperature-based face images.
   a. Multimodal
   b. Multisensory
   c. Multifactor
   d. Multifusion

5. _____ is the act of checking for the presence of the constituents of a given pattern.
   a. Pattern Matching
   b. Pattern Recognition
   c. Covert Screening
   d. Extraction

Continued .....

6. Generally fingerprint patterns are differentiated based on the presence of zero, one or two delta regions respectively for _____, _____, and _____.
   a. Loops; whorls, arches
   b. Arches; loops; whorls
   c. Tented arches; whorls; loops
   d. Whorls; loops; arches

7. These are some popular standard face data sets, **EXCEPT**:
   a. FERET
   b. PIE
   c. ORL
   d. CASIA

8. The percentage of times the system correctly rejects a false claim of identity, is called _____.
   a. True Reject Rate
   b. True Accept Rate
   c. False Reject Rate
   d. False Accept Rate

9. Which of the following is a network authentication protocol that allows individual communicating over an insecure network to proof their identity to one another?
   a. Kerberos
   b. Anti-virus
   c. Firewall
   d. Single Sign On

10. Open System Interconnection (OSI) is a ISO standard for worldwide communications that defines a networking framework for implementing protocols in 7 layers. Which of the below is NOT one of the seven layers?
    a. Presentation
    b. Session
    c. Data Link
    d. Communication

Continued .....

SECTION B: Please attempt **FIVE** out of **SIX** questions only

Question 1:

a) List the **FIVE (5)** factors of authentication and provide an example for each of them.

[5 marks]

b) AAA Protocols are used in IP-based networking to control what computer resources users have access to and to keep track of the activity of users over a network. Explain the services in the AAA Protocols.

[3 marks]

c) Most organizations specify a password policy that sets requirements for the composition and usage of passwords. Suggest any **TWO (2)** ways to eliminate easily guessed passwords.

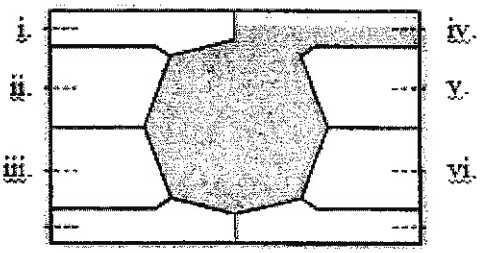
[2 marks]

Question 2:

a) A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. Discuss any **TWO (2)** approaches for the generation of OTPs.

[4 marks]

b) Integrated circuit (IC) chip defines capability of the smart card. Most chips consist of eight contact fields on the front face as illustrated in the diagram below. Label the fields.



[3 marks]

c) Define coercivity. With your best knowledge, explain the advantage of high coercivity.

[3 marks]

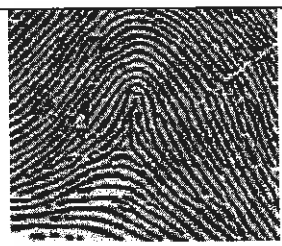
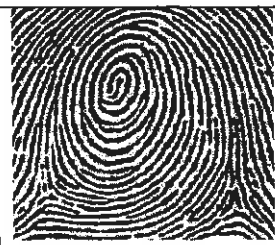
Continued .....

Question 3:

a) "Identification" and "Verification" are two common terms in biometric recognition. Differentiate both terms.

[2 marks]

b) Every individual has different types of fingerprint patterns. Three common types of fingerprint patterns are illustrated in the picture below. Name each of the patterns correctly. Fill in also the number of delta used to classify the fingerprint patterns.

Fingerprint patterns			
Name	(i)	(ii)	(iii)
No. of delta	(iv)	(v)	(vi)

[3 marks]

c) Fingerprint identification is one of the most important criminal investigation tools due to two features: their persistence and their uniqueness. How to relate the persistence and uniqueness with fingerprint identification? Justify the statement.

[3 marks]

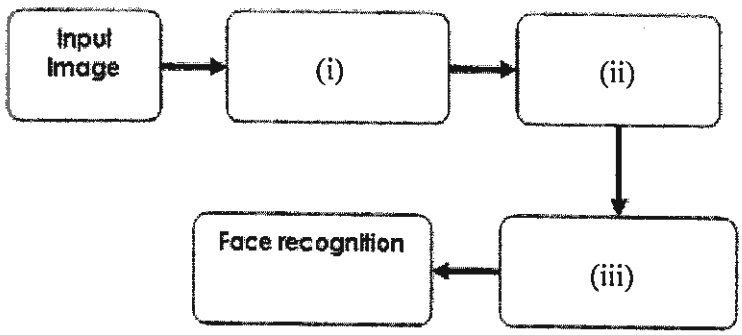
d) Matching is the process of acquiring new fingerprint image and matching against with the one that stored in database. This is to authenticate whether the user is the one who she/he claimed to be. However, there exists several challenges during the matching process. Identify the challenges.

[2 marks]

Continued .....

Question 4:

a) Name the activities in (i) - (iii) of a face recognition system in the following diagram.



[3 marks]

b) Principle Component Analysis (PCA) and Linear Discriminant Analysis (LDA) are two most popular and fundamental methods in face recognition. Based on your best understanding, explain the differences of these two methods. Illustrate the differences in diagrams as well.

[4 marks]

c) Why do you think that most of the Government agencies utilize the biometric authentication scheme instead of traditional password or token based authentication schemes? Which biometric modality they used normally? Why do you think they need to capture your biometric data?

[3 marks]

Question 5:

a) Do you think hand geometry recognition and palm-print recognition are similar? Discuss their strengths and weaknesses respectively.

[5 marks]

Continued .....

b) John was asked to apply biometric technology in his company's security system. Assuming you have adequate knowledge in biometric sector and he requested your assistance in explaining the following emerging biometric technology, how are you going to give a brief definition on each of them?

i. Ear shape recognition
ii. Nailbed identification
iii. Odor sensing

[3 marks]

c) There are two types of layered biometrics authentication procedures: Parallel layered and Serial layered. Explain the differences between both.

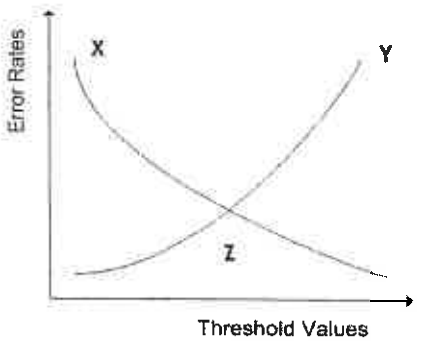
[2 marks]

Question 6:

a) "When designing Privacy-Sympathetic biometric systems, we should limit the retention of biometrics." Do you agree with this statement? Justify your answer.

[2 marks]

b) Graph below shows the performance evaluation metrics of biometric authentication system. Name and explain for the metrics X, Y and Z.



[3 marks]

Continued .....

c) Law enforcement is one of the five vertical markets for biometrics. Voice-scan is one of the attractive solutions in law enforcement to verify an individual is at home while under house arrest. Suggest another TWO (2) real life scenarios which utilize the biometrics in law enforcement.

[3 marks]

d) The Orange Book was the first guideline for evaluating security products for operating systems, which is issued by the National Computer Security Center (NCSC). List the criteria categories which have been covered by the Orange Book.

[2 marks]

End of Page